E-evidence Regulation and Directive Published

eucrim
European Law Forum: Prevention • Investigation • Prosecution

Thomas Wahl

News

After five years of negotiations, the Council and the European Parliament (EP) finally adopted the legislative acts that will **introduce a new system for the gathering of electronic evidence** in criminal proceedings in the EU. For the initial Commission proposal – the so-called e-evidence package – → eucrim 1/2018, 35-38. Eucrim has continuously reported on the progress of this legislative initiative and the stakeholders' criticism against it. After having reached political agreements in January 2023 (→ eucrim 1/2023, 45), the legislation was **published in the EU Official Journal** at the end of July 2023. The new rules on e-evidence consist of two legislative measures:

- Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (*O.J.* L 191, 28.7.2023, pp. 118–180);
- Directive (EU) 2023/1544 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings (*O.J. L 191, 28.7.2023, pp. 181–190*).

AUTHOR
Thomas Wahl
Senior Researcher
Max Planck Institute for the Study of Crime, Security and Law

Published in
2023, Vol. 18(2) eucrim pp 165 – 168
ISSN: 1862-6947
https://eucrim.eu

In order to apply the rules in a consistent manner and to provide time for implementation and compliance, the **Regulation applies from 18 August 2026**. The **Directive** must be **transposed** into the national laws of the EU Member States **by 18 February 2026**.

The **main aim** of the new EU legislation is to have in place an alternative – quicker and more efficient – mechanism to the existing international cooperation and mutual legal assistance tools in order to specifically address the problems stemming from the volatile nature of e-evidence and the "loss of location" aspect of stored data.

The Regulation lays down the rules under which an authority of a Member State, in criminal proceedings, may issue a European Production Order or a European Preservation Order and thereby (directly) order a service provider offering services in the Union and established in another Member State, or, if not established, represented by a legal representative in another Member State, to produce or to preserve electronic evidence regardless of the location of the data.

The Directive lays down the rules on the designation of designated establishments and the appointment of legal representatives of certain service providers that offer services in the Union, for the receipt of, compliance with and enforcement of decisions and orders issued by competent authorities of the Member States, for the purposes of gathering electronic evidence in criminal proceedings.

Summary

The following summarises the key features of the pieces of legislation by way of "Q&A":

Who is the addressee of the Regulation?

The Regulation applies to **service providers which offer services in the Union**. These notions are defined broadly.

For the purposes of the Regulation, a **service provider** is anyone providing one or more of the following categories of services (except for financial services):

- Electronic communication services, such as:
  - internet access services,
  - interpersonal communications services (e.g., messaging services, email services and internet telephony services);
- Internet domain name and IP numbering services, such as IP address assignment, domain name registries, and related privacy and proxy services;
- Other information society services which enable users to communicate with each other, or to store or otherwise process data, such as social networks, online marketplaces and other hosting service providers.

"Offering services in the Union" means:

- enabling natural or legal persons in a Member State to use the aforementioned services; and
- having a *substantial connection*, based on specific factual criteria, to the Member State referred to in the first point; such a substantial connection is to be considered to exist where the service provider has an establishment in a Member State, or, in the absence of such an establishment, where there is a significant number of users in one or more Member States, or where there is targeting of activities towards one or more Member States.

What is the scope ratione materiae?

- European Production Orders and European Preservation Orders may be issued only in the framework and for the purposes of **criminal proceedings**, and for the execution of a custodial sentence or a detention order of at least four months, following criminal proceedings. It is a condition that the sanction was not imposed by a decision that was rendered in absentia, in cases where the person convicted absconded from justice. Such orders may also be issued in proceedings relating to a criminal offence for which a **legal person** could be held liable or punished in the issuing State. Considering that legal notions of EU law are to be interpreted autonomously, "criminal proceedings" in this context could also mean administrative fine proceedings against corporates in which offences are at issue; this mainly concerns countries that do not know a corporate criminal law, such as Germany.

What are European Production and Preservation Orders?

The **Production Orders** allow law enforcement authorities in one EU Member State to request electronic data from service providers (established or represented in another EU Member State) and hand them over.

Preservation Orders can be issued by law enforcement authorities to oblige service providers to preserve electronic data that can later be requested for production, so that the data are prevented from being deleted or overwritten.

Which data are covered?

European Production and Preservation Orders can be issued for **subscriber, traffic, and content data** as traditionally defined (see also Art. 3(9), (11), and (12) of the Regulation). In addition, the Regulation introduces a fourth category of data, i.e., "**data requested for the sole purpose of identifying the user**". This category is defined as "IP addresses and, where necessary, the relevant source ports and time stamp, namely the date and time, or technical equivalents of those identifiers and related information, where requested by law enforcement authorities or by judicial authorities for the sole purpose of identifying the user in a specific criminal investigation".

The Regulation only applies to data that has already been stored, i.e., it does **not** apply to data allowing **live monitoring** and data that will be created in the future.

Who can issue the Orders?

- A **judge**, a **court**, or an **investigating judge** competent in the criminal case can issue all kinds of orders for all types of data that can be requested as electronic evidence (see supra);
- **Other designated investigating authorities** in criminal proceedings can also issue orders, but they must be **validated** by the judicial authorities referred to in the first point before transmission;
- **Public prosecutors** can issue European Production Orders to **obtain subscriber data and "data requested for the sole purpose of identifying the user"** (see above) as well as European Preservation Orders. For such orders, the public prosecutor is also a competent authority to validate orders from other investigating authorities (in addition to a judge, a court, or an investigating judge). If a public prosecutor wishes to obtain **traffic and content data**, his/her order must be **validated** by a judge, a court, or an investigating judge.

Which crimes can the Orders be issued for?

- A **European Production Order to obtain subscriber data or data requested for the sole purpose of identifying the user** (see above), may be issued for **all criminal offences** and for the execution of a custodial sentence or a detention order of at least four months;
- A **European Production Order to obtain traffic or content data** may be issued for criminal offences punishable in the issuing State by a **custodial sentence of a maximum of at least three years**, **or** – regardless of this threshold – a **specific set of offences** connected with cyber-crime, fraud relating to non-cash means of payment, terrorism and sexual abuse of children.
- A **European Preservation Order** may be issued for **all criminal offences**, "if it could have been issued under the same conditions in a similar domestic case", and for the execution of a custodial sentence or a detention order of at least four months.

Which deadlines apply?

In **regular cases**, the service provider must transmit the requested electronic evidence to the issuing authority within **10 days** following receipt of the European Production Order Certificate (EPOC). In **emergency cases**, the service provider has **8 hours** for transmitting the requested electronic data.

If **preservation** is requested, the service provider is obliged to preserve the data for **60 days**. The issuing authority can extend this period by an additional 30-day period.

What responsibilities does the issuing authority have?

- Looking at the most important instrument, i.e., the European Production Order, the issuing authority must **assess the necessity and proportionality** to the case at hand. It must take into account the rights of the suspect or the accused person in proceedings relating to a criminal offence and should only issue a European Production Order if such order could have been issued under the same conditions in a **similar domestic case**.
- The Order must include **specific information and justifications**, which are listed in Art. 5(5) of the Regulation.
- The issuing authority must **verify legal situations**, under which the issuance of European Production Orders is limited or excepted. This refers to (1) European Production Orders European Production Orders for all data categories if parallel criminal proceedings are ongoing in another Member State (***ne bis in idem* situations**), and (2) European Production **Orders for traffic and content data** if:
    - data are protected by **professional privilege** under the law of the issuing State (Art. 5(9) of the Regulation);
    - data protected by **immunities or privileges** under the law of the enforcing State, including data subject to rules on determination and limitation of criminal liability relating to freedom of the press and freedom of expression in other media under the law of the enforcing State (Art. 5(10) of the Regulation).
- In case of a European Production **Order for traffic and content data**, the issuing authority must **notify the enforcing authority** (i.e., the competent authority in the State, in which the service provider is established or its legal representative resides) **if the data subject or crime is outside the issuing State's jurisdiction** (cf. Art. 8 of the Regulation).
- The issuing authority must **review** the European Production Order if the service provider raises grounds not to enforce the Order (cf. Art. 10(5)-(9), Art. 17 of the Regulation).
- The issuing authority must **inform the targeted person** without undue delay about the production of data (cf. Art. 13 of the Regulation). Delaying and restricting the information for a limited period is possible in accordance with Art. 13(3) of Directive 2016/680).

What obligations do service providers have?

- Service providers offering services in the EU must **designate or appoint** at least one **addressee** for the receipt of, compliance with and enforcement of European Production and Preservation Orders (in accordance with Art. 3 of the Directive).
- Designated establishments or legal representatives of the service provider must be **staffed** with the necessary powers and resources to comply with the Orders (Art. 3(4) of the Directive).
- The service providers must **produce the data within the set deadlines** (see supra). If a European Preservation Order is received, data must be preserved without undue delay and be kept for the set period (see supra).
- The service provider has **information obligations** vis-à-vis the issuing and enforcing authority if it intends to raise objections to comply with the Orders (cf. Art. 10, Art. 11 of the Regulation).
- The service provider is subject to **possible sanctions for non-compliance**.
- The service provider must **ensure confidentiality**, secrecy and integrity of the data produced and preserved (cf. Art. 13(4) of the Regulation).

What rights do service providers have?

- The service provider can **seek clarification** from the issuing authority if the European Production Order is incomplete, contains manifest errors or insufficient information (cf. Art. 10(6) of the Regulation).
- The service provider can **raise two legal grounds not to comply** with a European Production Order:
  - Immunities and privileges (see supra and Art. 10(5) of the Regulation);
  - Conflict with an obligation under the applicable law of a third country (Art. 17(1), (2) of the Regulation).

What responsibilities does the enforcing authority have?

- The enforcing authority in the enforcing State is entitled to **evaluate orders** by the issuing state and to decide on their recognition, either when it was simultaneously notified (cf. supra and Art. 8 of the Regulation) or requested by the service providers, or during the enforcement procedure (if the service provider does not comply with a European Production or Preservation Order – Art. 16 of the Regulation).
- The enforcing authority can **raise** the following **grounds for refusal** (Art. 12 of the Regulation) **if it was notified** (i.e., cases of European Production Orders for traffic and content data and the data subject or crime are located outside the issuing State, cf. supra):
  - Immunities and privileges granted under the law of the enforcing State;
  - In exceptional situations, manifest breach of fundamental rights set out in Art. 6 TEU and the CFR;
  - Ne bis in idem;
  - Double criminality requirement not fulfilled unless the European Production Order concerns a listed offence with a specific threshold (Art. 12(1)(d) and Annex IV of the Regulation).
- Grounds for refusal pursuant to Art. 12 must be **raised within specific deadlines** (10 days following receipt of the notification in regular cases, and 96 hours following such receipt in emergency cases).
- Before deciding to raise a ground for refusal, the enforcing authority must **contact the issuing authority** and negotiate a solution.
- The enforcing authority must **ensure enforcement of legitimate orders** in accordance with the detailed rules stipulated in Art. 16 of the Regulation.

What rights does the targeted person/suspect have?

- A suspect or an accused person (or his/her lawyer) **can request the issuing** of a European Production or Preservation Order “within the framework of applicable defence rights in accordance with national criminal procedural law” (Art. 1(2) of the Regulation).
- The person whose data are being requested (targeted person) has the **right to be informed** of the production of data by the issuing authority unless a reason for delaying or restricting the information applies on the part of the issuing authority (Art. 13 of the Regulation).
- The targeted person must have the **right to effective remedies** against the order before a court in the issuing State (cf. Art. 18 of the Regulation).

How are conflicts of law resolved?

The Regulation provides for a special review procedure (Art. 17) if a service provider considers that compliance with a European Production Order would **conflict with an obligation under the law of a third country**. After the service provider had filed a "reasoned objection" (no later than 10 days after receipt of the EPOC) and duly informed the issuing and enforcing authorities, the issuing authority reviews its order and decides to uphold or withdraw it. If the issuing authority upholds the order, it must request a **review by a competent court of the issuing State**. The execution of the European Production Order is suspended pending completion of the review procedure at court. If the court has found that the law of the third country is applicable and prohibits disclosure of the data concerned, the court would not automatically lift the European Production Order but has to assess the interests at stake and take a **balancing decision**. The relevant factors are provided in Art. 17(6) of the Regulation.

Can service providers be sanctioned?

According to the **Regulation**, Member States must lay down **pecuniary penalties** if service providers infringe the rules on the execution of European Production and Preservation Orders. It must be ensured that pecuniary penalties of up to 2% of the service provider's total worldwide annual turnover can be imposed.

Infringements of the national rules transposing the **Directive** require Member States to lay down "**effective, proportionate and dissuasive penalties**" and take all measures necessary to ensure that they are implemented. In addition, Member States must annually report non-compliant service providers to the Commission.

Put in focus

The e-evidence Regulation and Directive is the result of a hard compromise found in trilogue negotiations between the European Parliament, the Council and the Commission–-. It reflects the difficult exercise to appropriately balance the interests for smooth law enforcement on the one hand and for adequate protection of fundamental rights and against misuse in favour of the individual on the other. The new legal instruments provide for more paths for law enforcement authorities to move the case forward despite obstacles prevalent in other jurisdictions.

Issues to reject the enforcement of orders from foreign jurisdictions are widely removed and, in essence, only exist in case of traffic and content data. The involvement of the enforcing State, for which the EP fiercely stood up, was limited at the end, since the notification requirement was made subject to several requirements. Given these limits and the tight deadlines, it can be questioned whether the Orders can be effectively reviewed. Practice will demonstrate whether the new rules to gather electronic evidence in the bloc are a progress and lead to the often proclaimed "paradigm shift" regarding cooperation in the EU.

In addition, it remains to be seen whether the EU's new e-evidence rules are apt for a model in other States or in multilateral conventions at the international level.

It is also noteworthy, that the e-evidence Regulation and Directive is one component of other recent EU regulations addressing online law enforcement. This includes, for instance, the EU Digital Services Act (DSA), which introduced responsibilities and a system of accountability and transparency for providers of intermediary services (→ eucrim 4/2022, 228-230), and Regulation 2021/784, which regulates the duties of care to be applied by hosting service providers to remove or disable access of terrorist content online (→ eucrim 2/2021, 95-97).

Criticism

Stakeholders fought until the end to stop the e-evidence Regulation. In an open letter of 12 June 2023, civil society, doctors, lawyers and journalists associations and internet service providers called on the EP to reject the "e-evidence package" since it risks to "severely undermine fundamental rights" and fails to provide legal certainty. It is regretted that the EP's improvements in first drafts did not last during negotiations with the Council. In addition, the associations criticised that the Regulation would set a terrible precedent for the level of protection when law enforcement authorities across the world order access to people's personal data from private entities in the EU. They found the following elements particularly concerning:

- Basically toothless notification system;
- Failure to account for national contexts with weakened rule of law and heightened risks of political repression;
- Poorly designed safeguards regarding professional secrecy and confidentiality;
- Limited right to effective remedies by insufficiently regulated "gag orders", weak rules for onward transfers and many barriers for individuals who defend themselves in front of a court.

In a press release of 13 June 2023, the European Broadcasting Union (EBU) commented: "Even though a few safeguards in relation to media freedom were introduced, we fear that the final text could still be misused to get hold of confidential data belonging to journalists."

NB: For a detailed analysis of the "e-evidence package" and its connection with other international developments → articles in related links.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union